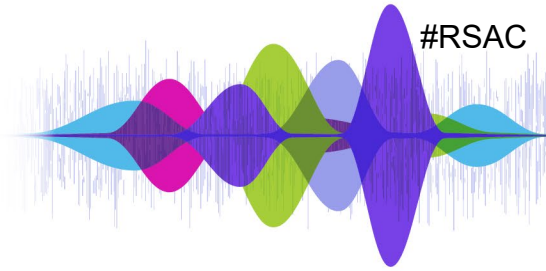
RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART3-R02

Futureproofing Cyber Ahead of the Next Wave of Emerging Tech

Jon France, CISSP, CGRC, ChCSP
CISO at ISC2
linkedin.com/in/jonfrance



Disclaimer

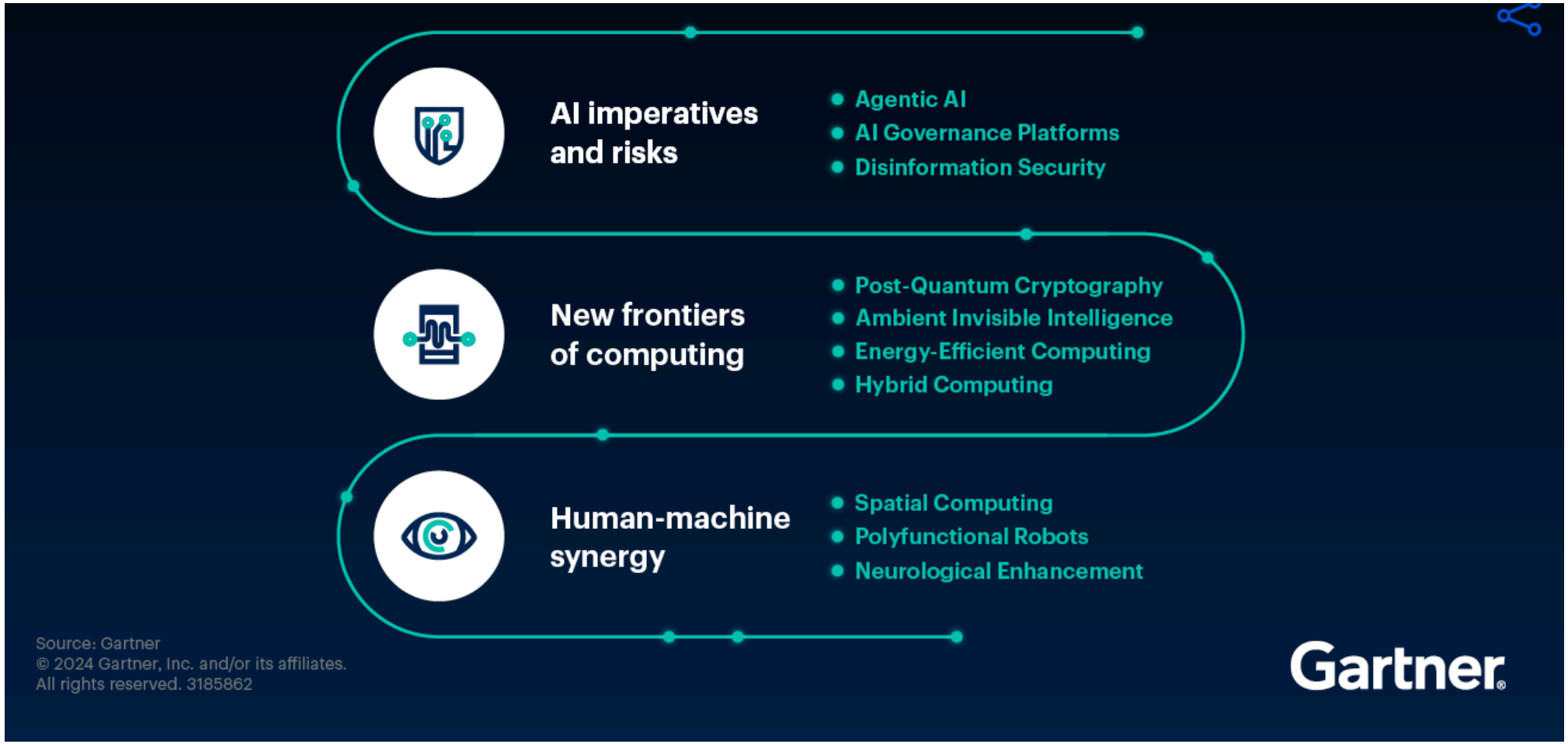
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

We'll explore how AI and Quantum computing are impacting the cybersecurity industry and what this means for cybersecurity professionals.

Gartner Top 10 Strategic Technology Trends for 2025

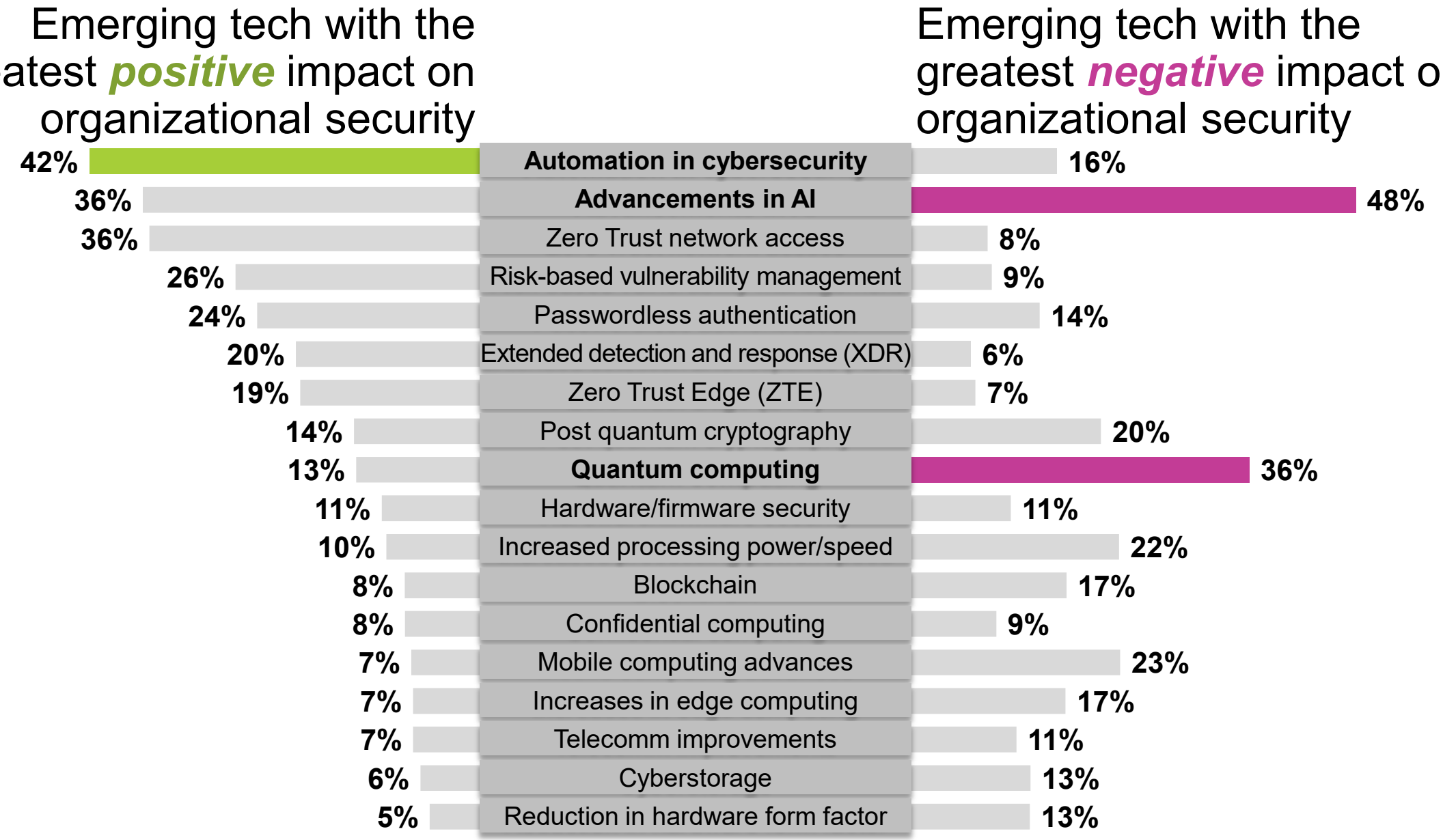


74%

of cybersecurity professionals say the threat landscape is the worst they've seen in 5 years

ISC2

Source: 2024 ISC2 Cybersecurity Workforce Study.

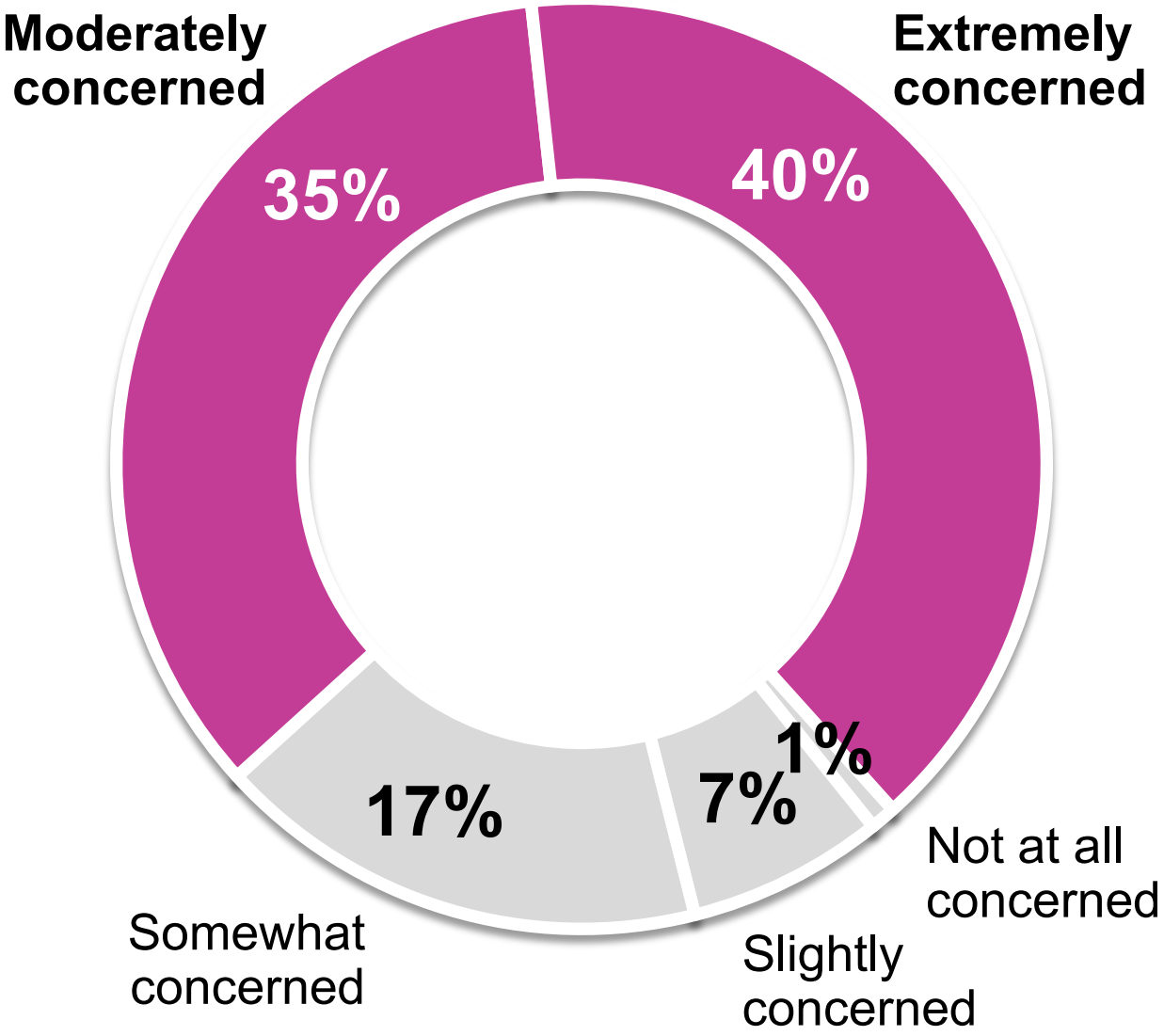

Emerging tech with the greatest positive impact on organizational security
Emerging tech with the greatest negative impact on organizational security
42% Automation in cybersecurity 16%
36% Advancements in AI 48%
36% Zero Trust network access 8%
26% Risk-based vulnerability management 9%
24% Passwordless authentication 14%
20% Extended detection and response (XDR) 6%
19% Zero Trust Edge (ZTE) 7%
14% Post quantum cryptography 20%
13% Quantum computing 36%
11% Hardware/firmware security 11%
10% Increased processing power/speed 22%
8% Blockchain 17%
8% Confidential computing 9%
7% Mobile computing advances 23%
7% Increases in edge computing 17%
7% Telecomm improvements 11%
6% Cyberstorage 13%
5% Reduction in hardware form factor 13%

Source: 2024 ISC2 Cybersecurity Workforce Study.

RSAC 2025 Conference

AI-driven risks and threats

Many Voices.
One Community.



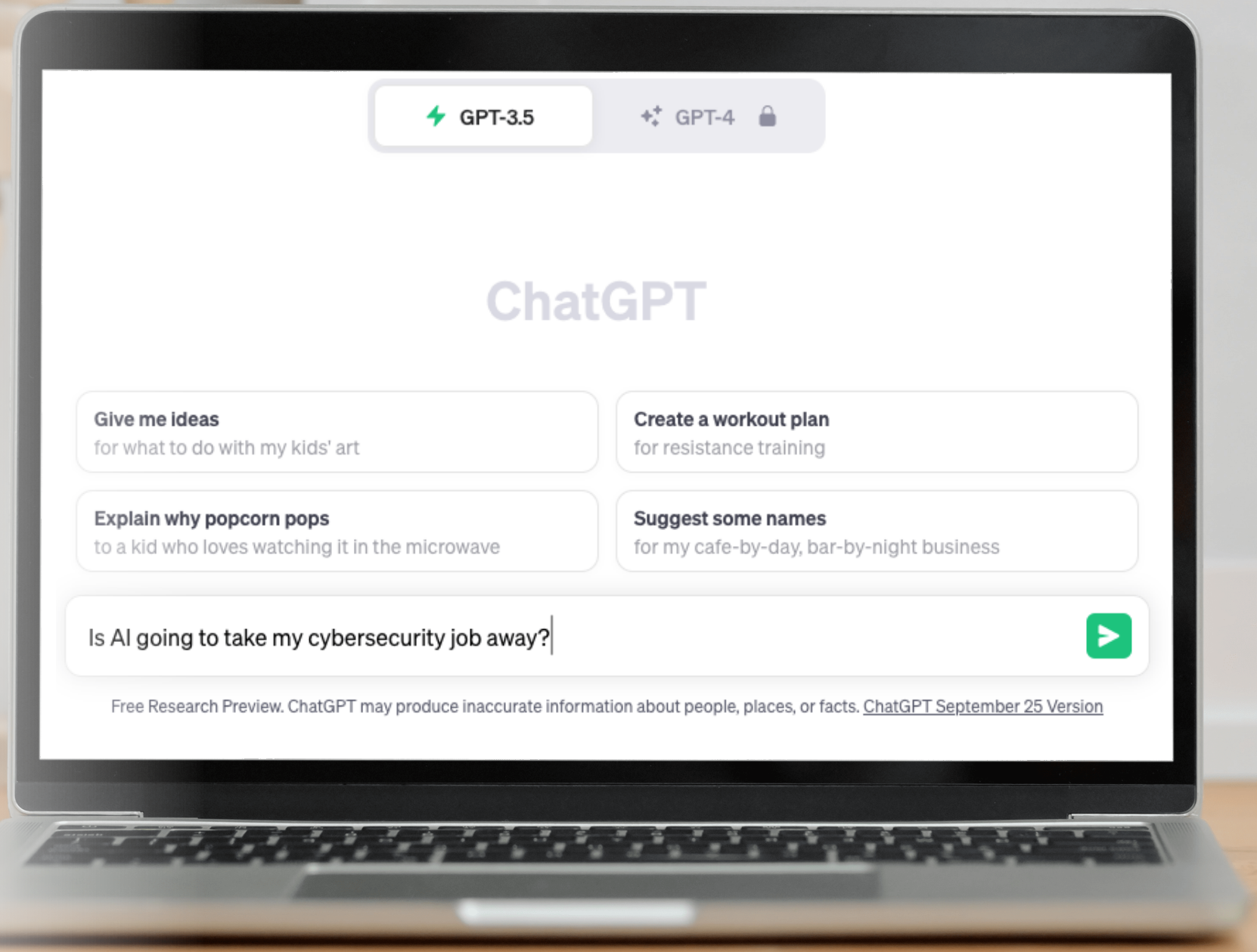
3 out of 4

survey participants are moderately to extremely concerned that AI will be used for cyberattacks or other malicious activities

Source: 2024 ISC2 Artificial Intelligence Survey.

67%

professionals agree that Gen AI will pose a significant threat for cybersecurity in the future.


GPT-3.5
GPT-4
ChatGPT
Give me ideas
for what to do with my kids' art
Create a workout plan
for resistance training
Explain why popcorn pops
to a kid who loves watching it in the microwave
Suggest some names
for my cafe-by-day, bar-by-night business
Is AI going to take my cybersecurity job away?
Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT September 25 Version

Source: 2024 ISC2 Cybersecurity Workforce Study.

Gen AI is being integrated into organizations, and most have use policies

45% of pros say Gen AI is built into the cybersecurity tools they use

64% say their organizations have implemented Gen AI in other parts of the organization

Source: 2024 ISC2 Cybersecurity Workforce Study.

Cyber pros see the positives of AI

54%
say advancements in AI will be more helpful than hurtful to cybersecurity

66%
see securing Gen AI as a career growth opportunity

80%
believe their cybersecurity skill set will be more important in an AI-driven world

71%
believe Gen AI will allow them to do their job more efficiently

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

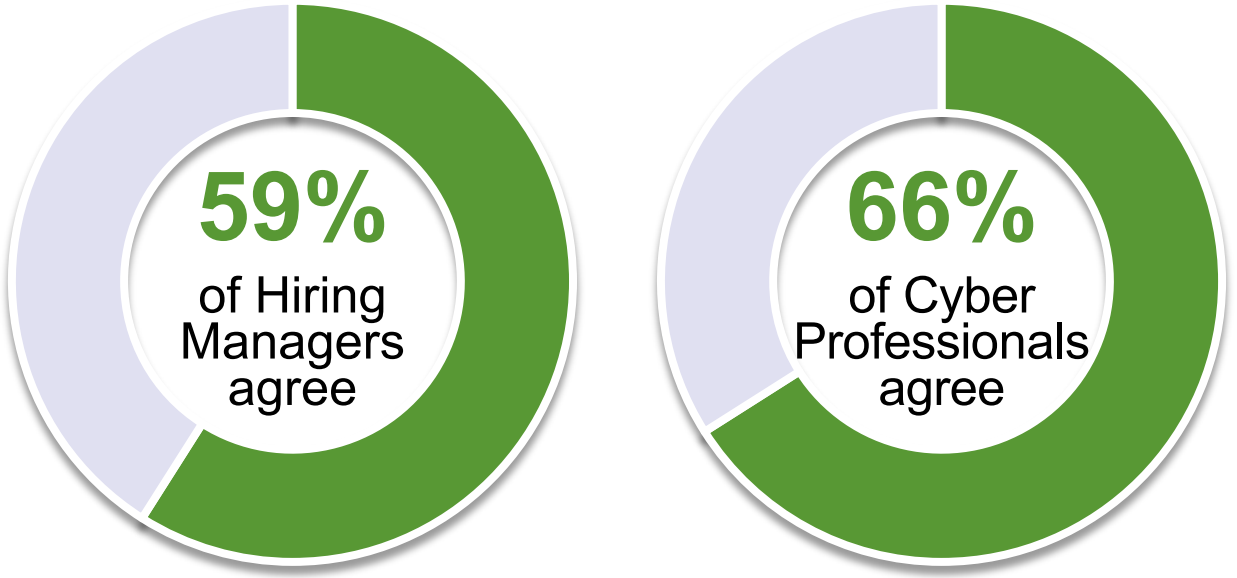
34%

of cybersecurity pros have identified a lack of AI cyber skills within their teams, a significant skills gap.

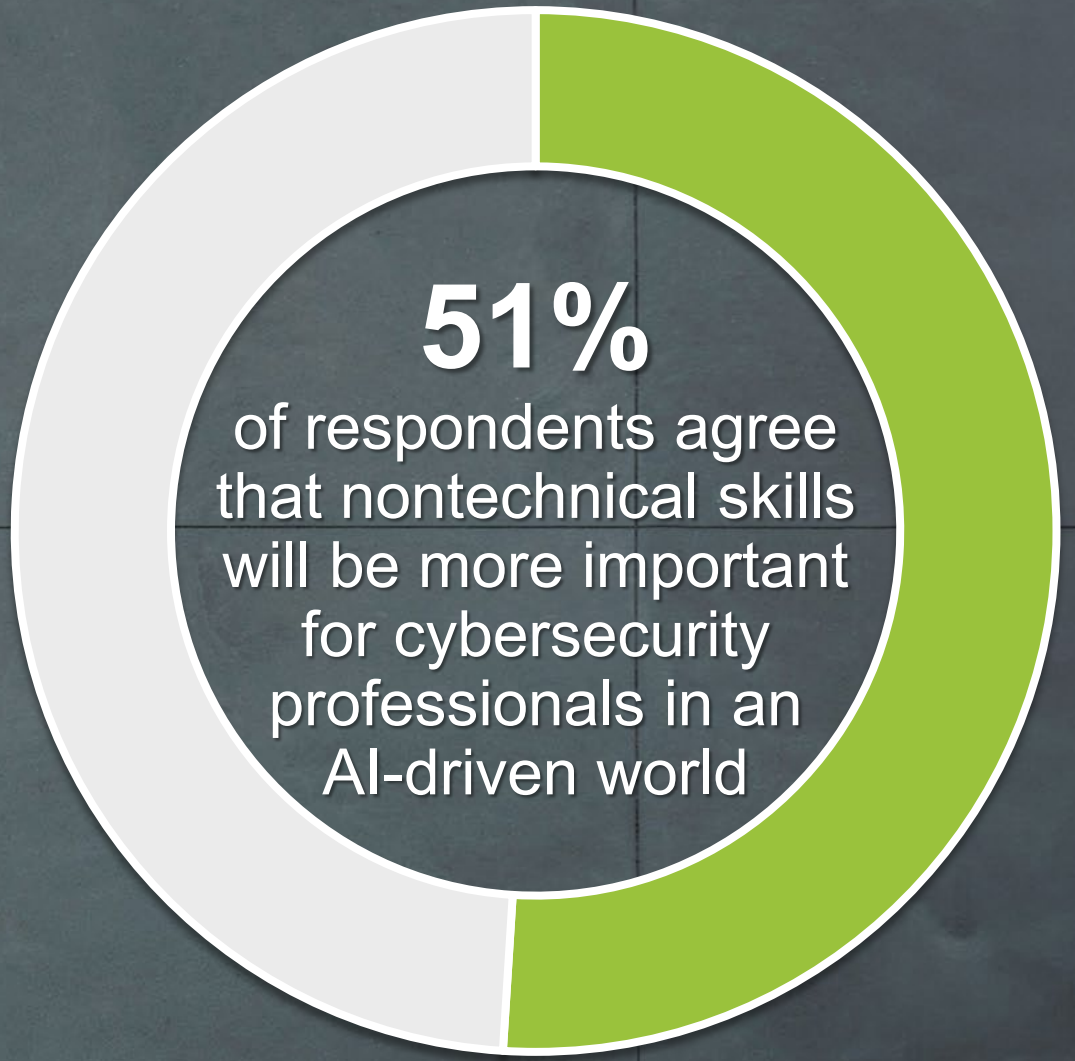
ISC2

Skills needed for AI/ML are somewhat unclear

"I don't know enough about Gen AI to identify the skills I'll need to succeed in an AI-driven world."

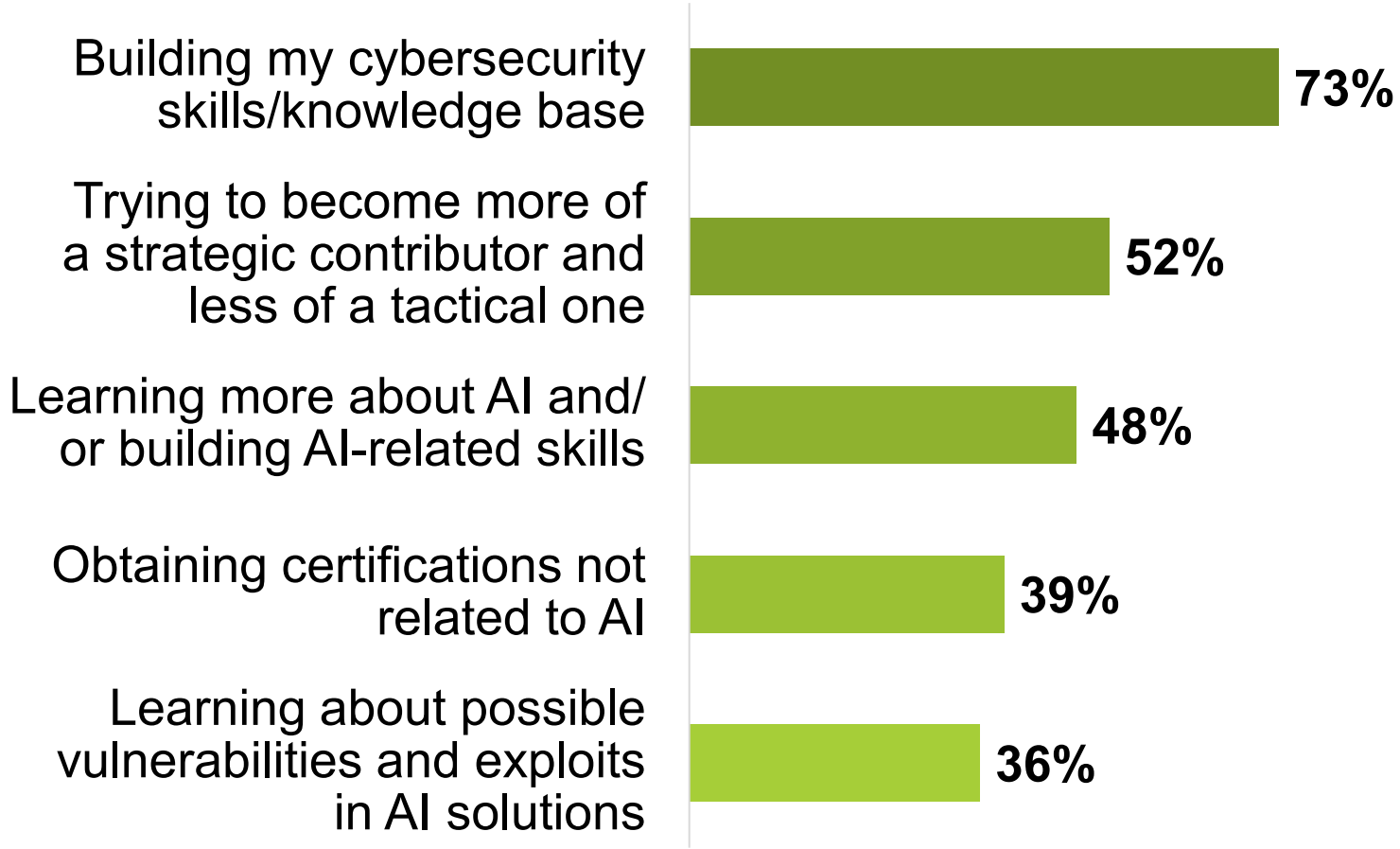


Source: 2024 ISC2 Cybersecurity Workforce Study.


51%
of respondents agree that nontechnical skills will be more important for cybersecurity professionals in an AI-driven world

Source: 2024 ISC2 Cybersecurity Workforce Study.

Cyber pros are future-proofing their skills for AI


Building my cybersecurity skills/knowledge base
73%
Trying to become more of a strategic contributor and less of a tactical one
52%
Learning more about AI and/or building AI-related skills
48%
Obtaining certifications not related to AI
39%
Learning about possible vulnerabilities and exploits in AI solutions
36%

Two-thirds

believe their skills will be complemented, not threatened, by AI

Source: 2024 ISC2 Cybersecurity Workforce Study.

RSAC™ 2025 Conference

Secure AI Adoption

Develop formal AI strategy

AI Security Policies

Are your organization's goals and objectives tied to AI security?

Who will be responsible for overseeing and managing AI security policies?

AI Risk Management

Are you aware of the security risks associated with your AI systems?

What is the potential impact if an AI system is breached?

AI Compliance & Regulations

How are you ensuring compliance with relevant regulations and standards?

Are there regulatory and industry guidelines for AI security that must be followed?

Source: 2024 ISC2 Artificial Intelligence Survey.

Who is responsible for secure AI?

Business Leaders

Security strategy and compliance

Threat intelligence and risk management

Developers/ DevOps

Code analysis and threat detection

Vulnerability assessment

Operational Personnel

Incident response automation

User and entity behavior analytics (UEBA)

Security Professionals

Threat detection and response

AI enhanced endpoint protection

Source: 2024 ISC2 Artificial Intelligence Survey.

Cyber pros should collaborate with the Board to manage AI risks while fostering innovation for competitive advantage.

RSAC 2025 Conference

Cyber Risks of Quantum Computing

Many Voices.
One Community.

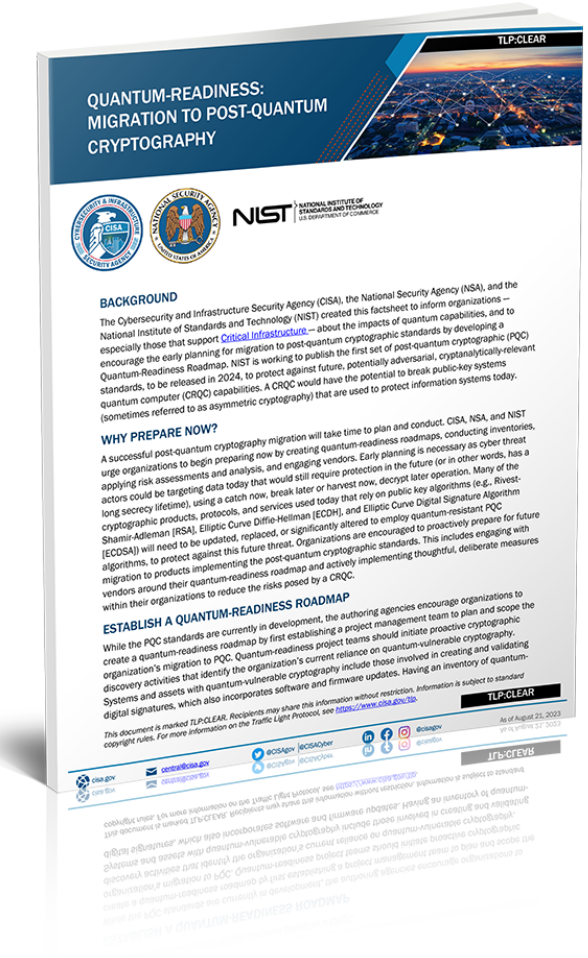
There’s an urgent need for quantum-savvy cybersecurity professionals

36%

say quantum computing will have a **negative** effect on security in their organizations.

Source: 2024 ISC2 Cybersecurity Workforce Study

Recent Quantum news



NIST Search NIST Menu

NEWS

NIST Releases First 3 Finalized Post-Quantum Encryption Standards

August 13, 2024

- NIST has released a final set of encryption tools designed to withstand the attack of a quantum computer.
- These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy.
- NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

ETSI

Back

ETSI/IQC Quantum Safe Cryptography Conference 2025

QiC | Quantum Industry Coalition

Preparing for Quantum Computing

Preparing as a cyber profession

Education/awareness – understanding, interpreting and then articulating

Skilled workforce

Preparing your organization

Get ready for change - inventory, risk assess, plan

Start moving for high value, continue to refine

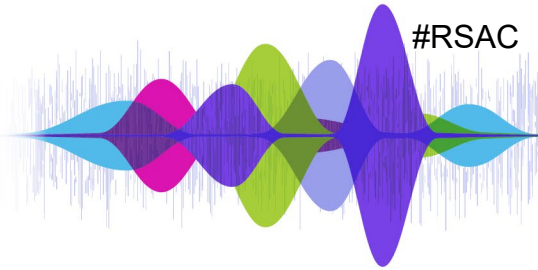
Complete the rest

RSAC™ 2025 Conference

Looking Ahead

Many Voices.
One Community.

Apply what you have learned today



- Begin discussions about how AI is being leveraged at your organization
- Review existing AI policies at your organization and work to implement new policies
- Collaborate with leaders to create an AI security training plan for ongoing education on evolving AI skills and knowledge
- Have a basic understanding of what quantum computing is and how to explain it
- Prepare your organization for quantum as you would any other emerging technology

RSAC 2025 Conference

Many Voices.
One Community.

Any Questions?

Jon France, CISSP, CGRC, ChCSP

CISO at ISC2
linkedin.com/in/jonfrance